BANCA D'ITALIA
EUROSISTEMA

Dipartimento Mercati e sistemi di pagamento
Servizio Supervisione mercati e sistema dei pagamenti

La sicurezza nell'era del digitale: regole e cooperazione

Domenico Gammaldi
domenico .gammaldi@bancaditalia.it

ABI – Banche e Sicurezza 2016, Milano 26 e 27 maggio 2016

Agenda

1. Sfide alla sicurezza nell'era digitale
2. Cyber security e Banca d'Italia
3. Iniziative di cyber security: cooperazione e regolamentazione
4. Punti di attenzione e piano di azione

Sfide alla sicurezza nell'era digitale

Interazione tra sicurezza fisica e sicurezza logica

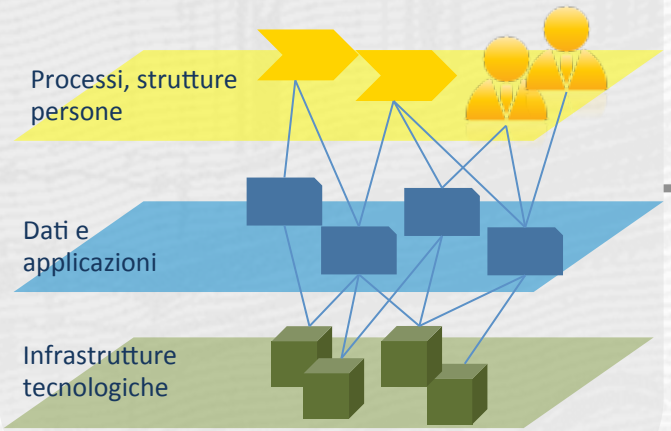
- Attacco cyber con distruzione fisica dell'obiettivo
- Attacco fisico per sfruttare vulnerabilità "logiche" e accedere al sistema informativo aziendale

Servizi di sicurezza informatica

Sistema di sicurezza fisica

- Posti di controllo
- Videosorveglianza
- Aree sensibili
- …

Enterprise



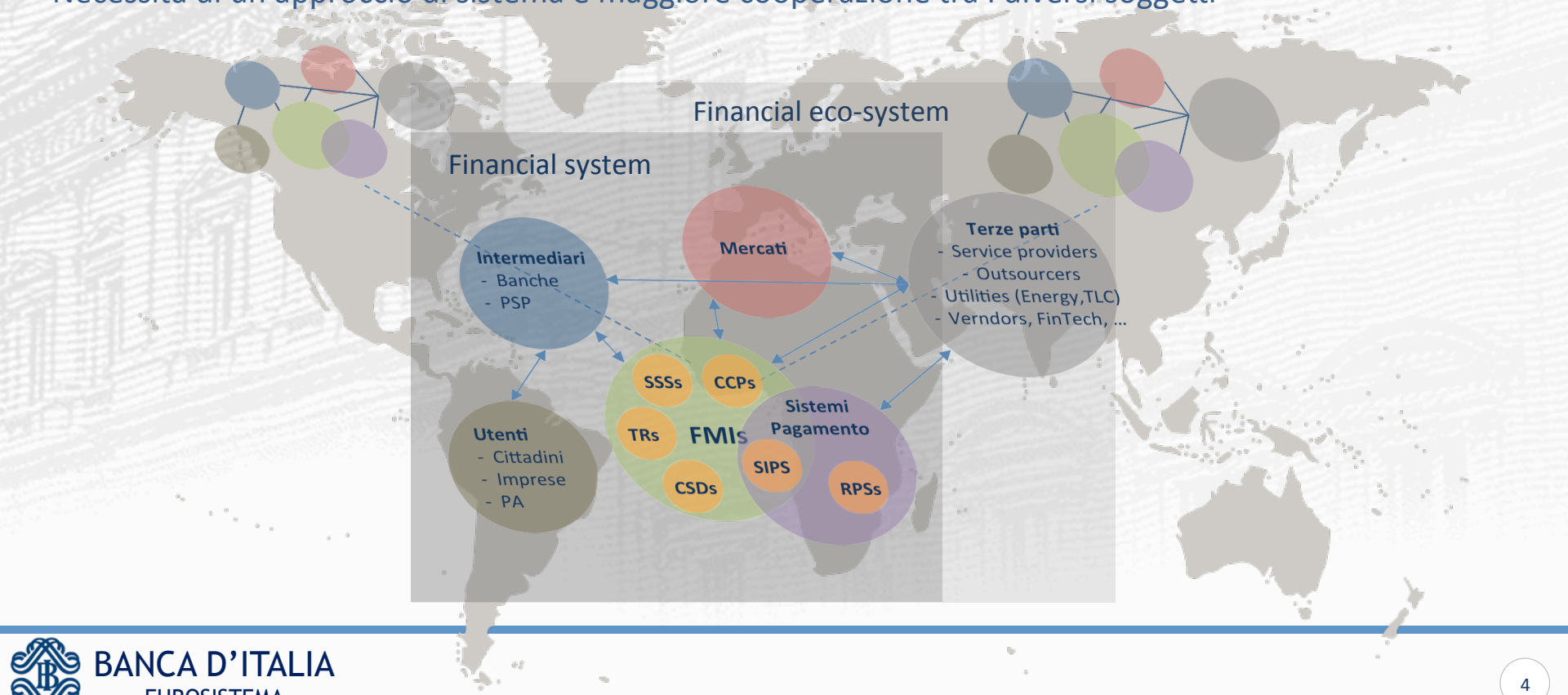
Sistema di sicurezza informatica

- Difesa perimetrale
- Segregazione
- Virtualizzazione
- Protezione End-Point
- …

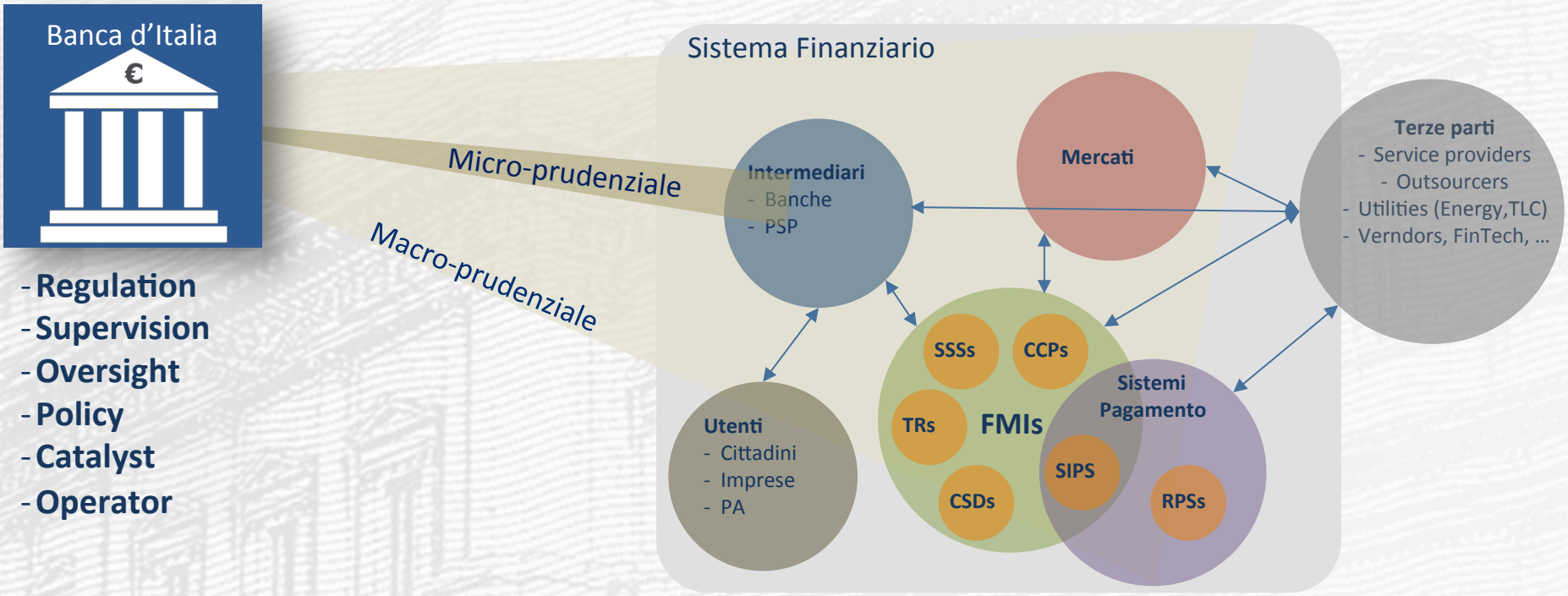
Servizi di sicurezza fisica

Dipendenze inter-settoriali e cross-border

- Interdipendenze critiche sui piani tecnologico e finanziario (nazionale e *cross-border*)
- Connessioni con altri settori critici di servizi essenziali (Energia e TLC *in primis*) e terze parti (*outsourcer*)
- Mutue vulnerabilità condivise attraverso il cyberspace (Rischio di interdipendenze)
- Rapida propagazione di shock (contagio) con potenziale impatto sulla stabilità finanziaria
- Necessità di un approccio di sistema e maggiore cooperazione tra I diversi soggetti



Cyber security e Banca d'Italia



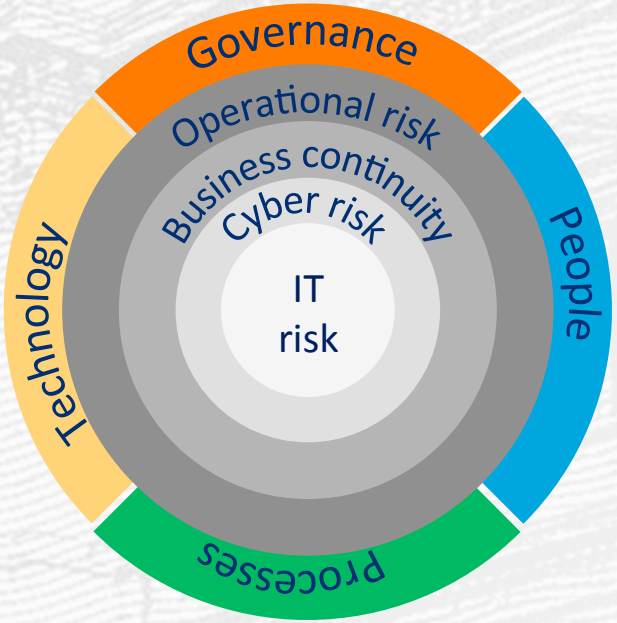
Assicurare la stabilità finanziaria e la fiducia del pubblico nel sistema finanziario

- Valutare e monitorare la capacità di cyber resilience del sistema finanziario
- Favorire la cooperazione tra i diversi portatori d'interesse (approccio di sistema e multi-stakeholder)
- Promuovere la diffusione della cultura del rischio
- Potenziare le capacità di risposta e di gestione delle crisi (comunicazione e coordinamento)
- Sostenere le iniziative nazionali e internazionali in tema di cyber security

Approccio di regolamentazione e di supervisione dei rischi cyber

Regolamentazione e policy

- Disposizioni di vigilanza per le banche (2015)
- Disposizioni di sorveglianza su RPS (2012)
- Linee guida per la continuità operativa (2014)
- CODISE



Supervisione

On-going e puntuale

rafforzare

valutare

Cyber security capabilities

assicurare

Cyber security objectives

Cyber security e Banca d'Italia

Rilevanza del fattore umano

- Focus su attori di minaccia (fattore antropico della minaccia) oltre a vettori e obiettivi
- Vulnerabilità non solo tecnologiche, ma **umane** e di processo

Vulnerabilità

Utenti
- **Clienti**
- **Dipendenti**

Top & senior management

Insider

Terze parti
- **Consulenti**
- **Fornitori**

Minacce

Soggetti <u>politicamente</u> motivati

- Attivisti, Gruppi antagonisti, Nation-state proxies
- Motivazione ideologica, geopolica, economica (spionaggio industriale)
- Potenziale impatto **SISTEMICO**

Soggetti <u>economicamente</u> motivati

- Organizzazioni e Singoli (Cyber criminali)
- Motivazione prevalentemente economica (profitto)
- Impatto **NON SISTEMICO**

Iniziative di cyber security: cooperazione e regolamentazione

Sicurezza? Non solo cyber (Securepay e PSD2)

Ambito di intervento

Europeo

- Armonizzazione di regole per favorire lo sviluppo e la sicurezza del mercato interno dei servizi di pagamento.

Obiettivi

- Assicurare la sicurezza dei pagamenti on-line attraverso l'emanazione di raccomandazioni tecniche (strong authentication, risk assessment, transactions authorisation and monitoring, user profiling and alerting)
- Pervenire ad un framework armonizzato per la segnalazione dei major incident per le banche e i prestatori di servizi di pagamento, i gestori di sistemi di pagamento al dettaglio , le carte di credito/debito)
- Migliorare la comunicazione e lo scambio informativo a livello europeo tra le autorità e con i soggetti vigilati

Attività

- Linee guida sui pagamenti online

- Sviluppo di *Regulatory Technical Standard* sulle **4 dimensioni della sicurezza previste dalla PSD2**
  i. RAPPORTI CON L'UTENZA: autenticazione forte e comunicazione sicura
  ii. RAPPORTI TRA INTERMEDIARI: comunicazione sicura tra PSP e TPP
  iii. AZIENDALE: processi operativi
  iv. SISTEMICA: incident reporting e info-sharing tra autorità (cfr. NIS directive)

CPMI-IOSCO: Guidance on cyber resilience for FMIs

Ambito di intervento

Internazionale

- Capacità di resilienza atti attacchi cyber in ottica di continuità operativa delle infrastrutture di mercato quali soggetti di rilevanza sistemica per la stabilità finanziaria e la crescita economica

Obiettivi

- Analizzare la rilevanza delle minacce cyber per le infrastrutture di mercato e per le autorità di supervisione
- Proporre delle linee di indirizzo per il potenziamento della capacità di cyber resilience delle infrastrutture di mercato in linea con CPMI-IOSCO Principles for FMIs (2012).
- Rafforzare la cooperazione e lo scambio informativo tra le autorità di supervisione

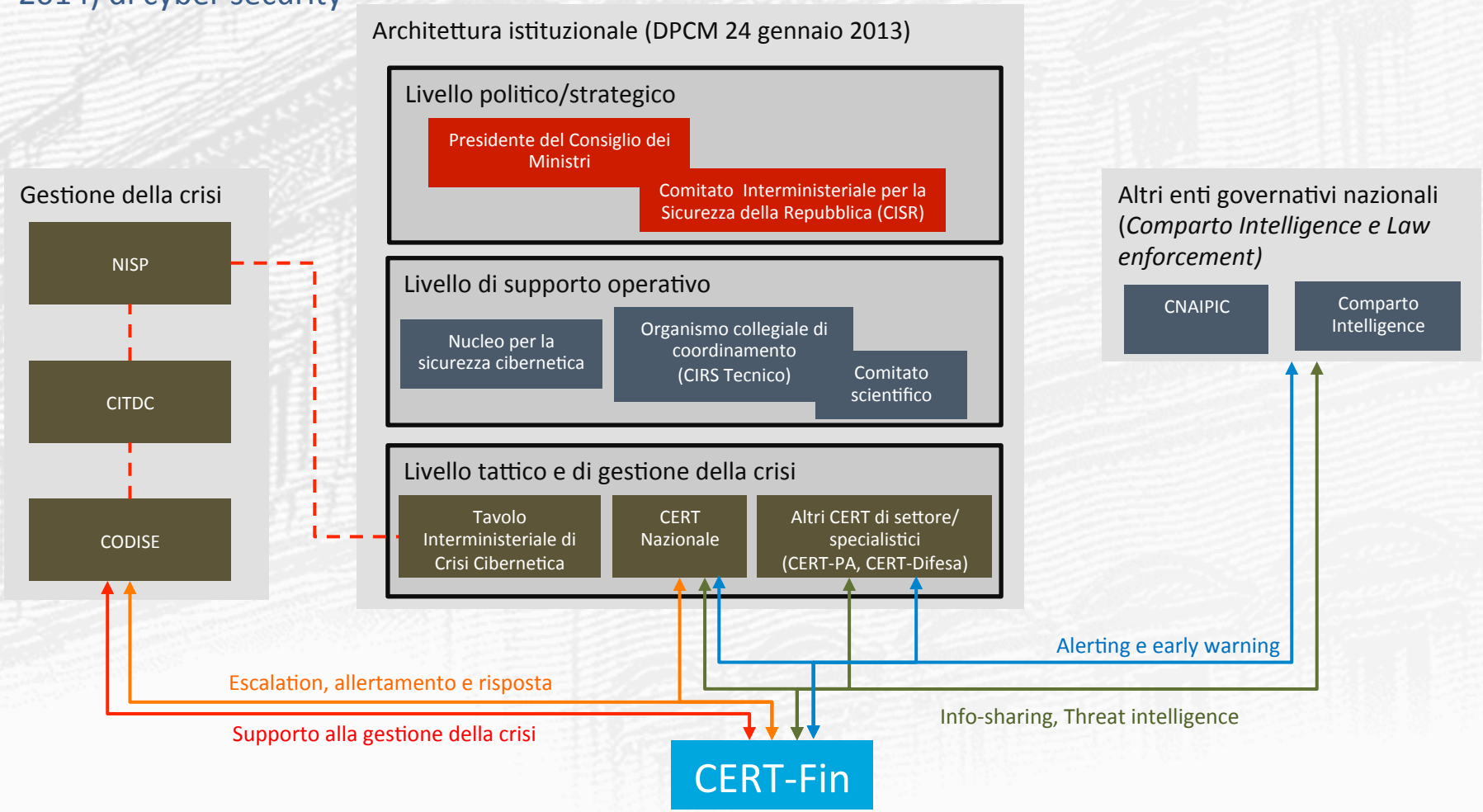
Elementi chiave

- Assunzione dell'impossibilità di prevenire l'attacco e necessità di assicurare continuità operativa dei servizi critici anche in casi estremi, ma plausibili (*Worst case scenario*: attacco avanzato e persistente con compromissione dell'integrità dei dati e dei sistemi)
- **5 aree principali** (*governance, identification, protection, detection, recovery*) e **3 componenti trasversali** (*testing, situational awareness, learning and evolving*) che i framework di gestione del rischio cyber delle FMIs devono indirizzare
- NO uno standard tecnologico, NO ulteriori principi rispetto ai PMFIs ma un loro supplemento per la corretta gestione dei rischi cyber
- Già svolta la consultazione pubblica; **pubblicazione definitiva prevista per fine giugno 2016**

Iniziative di cyber security: cooperazione e regolamentazione

La cooperazione: l'iniziativa CERT-FIN in Italia

- Coerenza con l'architettura istituzionale (DPCM 24 gen 2013) e la strategia nazionale (DPCM 27 gen 2014) di cyber security



Iniziative di cyber security: cooperazione e regolamentazione

La cooperazione: l'iniziativa CERT-FIN in Italia

Ambito di intervento

Nazionale

- Potenziamento delle capacità di cyber resilience del settore finanziario italiano. Prevalente prospettiva di sicurezza nazionale e del principio di sussidiarietà della norma

Obiettivi

- Contribuire all'attuazione della Strategia nazionale di cyber security (DPCM 27 gennaio 2015)
- Condividere informazioni e analisi su minacce, vulnerabilità, eventi cyber
- Migliorare la comunicazione e il coordinamento in caso di incidenti su larga scala in accordo con quanto già svolto dal CODISE per la continuità operativa e la gestione delle crisi
- Promuovere la cooperazione Pubblico-Privato
- Promuovere e diffondere la cultura di *cyber security*

Caratteristiche

- **Iniziativa cooperativa** promossa dalla Banca d'Italia in collaborazione con l'Associazione Bancaria Italiana
- Coinvolgimento attivo delle Autorità (promozione della cooperazione pubblico-privato)
- Adesione su base **volontaria** e **aperta** a tutte le istituzioni finanziarie
- **Separazione dei ruoli e regole** per l'infosharing

Iniziative di cyber security: cooperazione e regolamentazione

La cooperazione: l'iniziativa CERT-FIN in Italia

- Governance su più livelli con coinvolgimento attivo della Banca d'Italia
- Modello organizzativo a **"Campus"** in ottica collaborativa e di riuso di competenze acquisite
- Adesione regolamentata e orientamento al servizio

Governance

Livello Strategico

Livello Tattico/Operativo

Organizzazione

Direzione e coordinamento CERT-Fin
(Componente accentrata)

Membri del Campus: CERT/SOC di alcuni soggetti aderenti
(Componente decentrata)

1. **Convenzione Banca d'Italia - ABI**
2. **Regolamento di adesione (membri del campus, membri della *constituency*)**
3. **Eventuale potenziamento dei servizi in ottica campus (membri del campus)**

Punti di attenzione e piano di azione

Recepimento Direttive NIS e PSD2

- Il 17 maggio u.s., Il Consiglio europeo ha confermato l'adozione della Direttiva secondo l'accordo raggiunto con il Parlamento europeo a dicembre 2015. Rimane l'approvazione in seconda lettura del Parlamento. Prevista entrata in vigore ad agosto 2016
- Recepimento della NIS con particolare riferimento agli aspetti di cooperazione tra gli Stati Membri e obblighi di sicurezza per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, l'assistenza sanitaria e la finanza) e i fornitori di servizi digitali (mercati online, motori di ricerca e servizi di cloud) tra cui l'*incident reporting* all'autorità competente
- **Necessità di recepimento coordinato per operatori finanziari**

Cooperazione tra istituzioni

- Definizione di efficaci e lineari meccanismi di coordinamento tra le diverse istituzioni nel rispetto delle competenze specifiche (G7, G20, FSB, EBA, Commissione UE)

Attivazione di linee guida e raccomandazioni

- Le linee guida e le raccomandazioni provenienti dai diversi tavoli attivi sul tema potrebbero richiedere azioni di regolamentazione, supervisione o di policy

Armonizzazione tra le diverse iniziative

- Vari livelli (domestico, europeo, internazionale); diversi stakeholder e obiettivi; livello di maturità differenti